

**NORMAN®**



# **WEB QUARANTINE USER GUIDE**

VERSION 4.3



# **WEB QUARANTINE**

## **USER GUIDE**

Version 4.3



The content of this manual is for informational use only and is subject to change without notice. Neither Norman nor anyone else who has been involved in the creation or production of this manual assumes any responsibility or liability for any errors or inaccuracies that may occur in this manual, nor for any loss of anticipated profit or benefits, resulting from the use of this manual.

This manual is protected by copyright law and international treaties. Your right to copy this manual is limited by copyright law and the terms of the software license agreement. As the software licensee, you may make a reasonable number of copies or printouts, provided it is for your own use. Making unauthorized copies, adaptations, compilations or derivative works for any type of distribution is prohibited and constitutes a punishable violation of the law.

Any references to names of actual companies, products, people and/or data used in screenshots are fictitious and are in no way intended to represent any real individual, company, product, event and/or data unless otherwise noted.

Norman Email Protection, Norman Virus Control and NVC are trademarks of Norman ASA. Windows, Windows NT, Windows 2000, IIS, Internet Information Server and Data Access Components are either registered trademarks or trademarks of Microsoft Corporation. Platypus, RODOPI, Emerald, EcoBuilder, Logisense and Worldgroup are trademarks of their respective owners. All other products or services mentioned in this document are identified by the trademarks or service marks of their respective companies or organizations.

Norman Email Protection is based on the Professional Internet Mail Services product licensed from the University of Edinburgh.

Certain algorithms used in parts of this software are derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm.

Copyright © 1995-2006 Norman ASA

Norman ASA, PO Box 43, 1324 Lysaker, Norway

For more information, contact your local Norman subsidiary, contact details found at

[www.norman.com/Partner/Subsidiaries\\_and\\_distributors/11229](http://www.norman.com/Partner/Subsidiaries_and_distributors/11229)

January 2006

# Table of Contents

<b>Chapter 1: Introduction</b>	<b>1</b>
About this User Guide	2
Selecting Pages	2
Selecting Email from Lists	2
Open email	2
Select multiple emails	2
Mouse Actions	2
Note Icons	3
Starting a WebQuarantine Session	4
Logging In	4
The NEP WebQuarantine Interface	5
Searching Quarantine	8
Paging	8
Navigating List Pages	8
<b>Chapter 2: Quarantine</b>	<b>9</b>
Managing Your Quarantined Mail	9
Quarantine Categories	10
False Positives	10
Releasing Email from Quarantine	11
Deleting and Purging Quarantined Email	12
Quarantine Reports	12
Releasing or Deleting Quarantined Email from the Quarantine Report	13

<b>Chapter 3: Settings</b>	14
Options	15
Specify the Number of Messages to be Displayed in Lists	15
Email Filters	16
Modifying your Anti-Spam Filter Settings	17
To choose the level of Spam Filtering:	17
Modifying your Anti-Virus Filter Settings	18
To turn Virus Filtering on or off:	19
To modify Virus notification settings:	19
Forbidden Attachments	19
Blocked Senders and Trusted Senders	20
Adding Addresses to Your Trusted List	20
Adding Addresses to Your Blocked List	21
Quarantine Report Settings	22
 <b>Chapter 4: Statistics</b>	 21
Account Statistics	21
Email Traffic for the Last 7 Days	22
See a daily breakdown of types of spam received	22
Email Traffic for the Last 8 Weeks	23
See a weekly breakdown of types of spam received	23
Email Traffic for the Last 12 Months	24
See a monthly breakdown of types of spam received	24
 <b>Glossary</b>	 25

# Chapter 1: Introduction

Norman E-mail Protection (NEP) WebQuarantine is an application that allows you to access and manage your quarantined email from anywhere in the world through the internet.

This user guide will walk you through each step of the tasks you can perform in NEP WebQuarantine.

## About this User Guide

This user guide assumes that you have a working knowledge of your computer and its operating system, including how to use a mouse.

The guide is structured in a series of tasks to help you learn the system as quickly as possible. If you want information on how to perform a task, refer to the Table of Contents. For explanations of terminology or acronyms related to email and email security, there is a Glossary at the back of the guide.

## Selecting Pages

Pages or buttons that you must click are displayed in bold in this guide. If you have to go through a series of pages to find a specific command, your instructions will list the pages in the order you need to access them.

For example:

To see your Trusted List, go to **Settings > Email Filtering > Trusted Senders**

## Selecting Email from Lists

NEP WebQuarantine uses standard conventions for selecting specific email messages from lists.

### Open email

- Click once on an email to open it.

### Select multiple emails

- Select the checkboxes of more than one email to perform an action on multiple emails (such as releasing email from quarantine or deleting)

## Mouse Actions

These terms are used to describe which mouse button to use:

Click	Click the left mouse button
Right-click	Click the right mouse button
Double-click	Click the left mouse button rapidly twice without moving the cursor

## Note Icons

We've put important notes related to the main text in the left margin. These icons indicate the importance of the note information:



Indicates that the note is something you must know and possibly act on.



Indicates extra information that will be especially helpful to you.



Indicates details that will help you perform a task, such as an alternative method or how the system will respond to your actions.



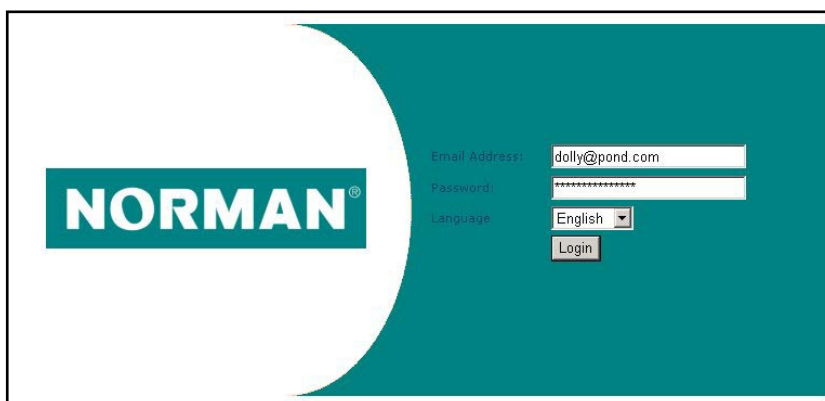
## *Starting a WebQuarantine Session*

NEP WebQuarantine requires you to identify yourself as a user with an email address and password. From the Login screen you can also change the language of the display.

### Logging In

To start a new mail session:

1. Open your internet browser and go to the URL provided by your ISP for your NEP WebQuarantine login page
2. Enter your email address and password
3. Click Login



The NEP WebQuarantine Login Screen

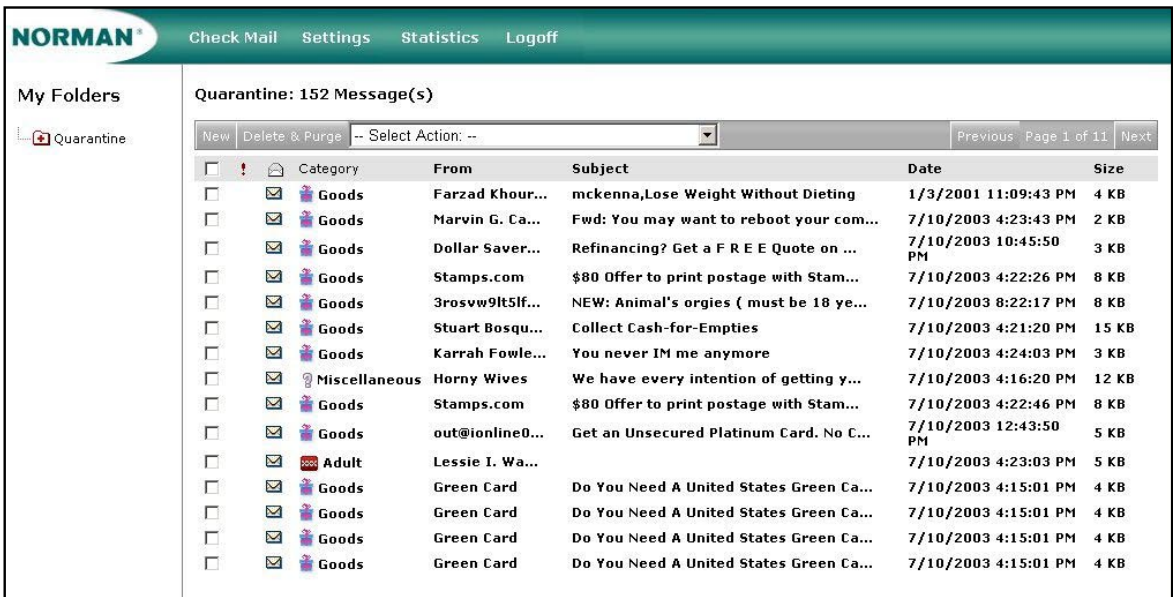
# The NEP WebQuarantine Interface

Use the navigation bar at the top of every screen to go to the corresponding window.



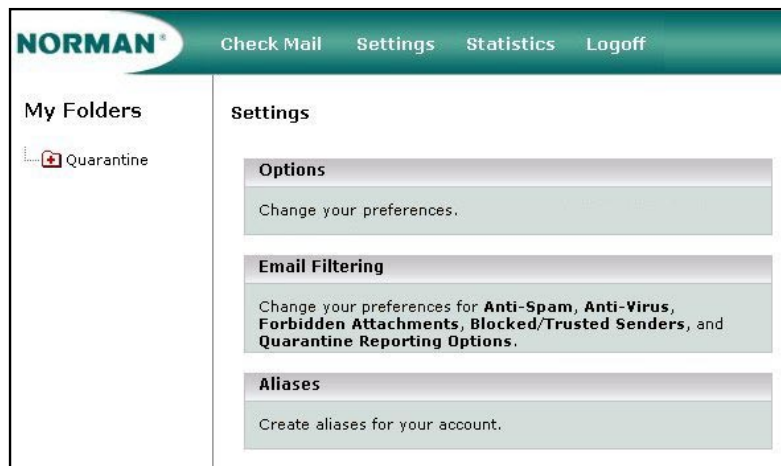
Navigation bar

**Check Mail:** Click **Check Mail** to display your quarantine and see if any new mail has been quarantined since you logged in.



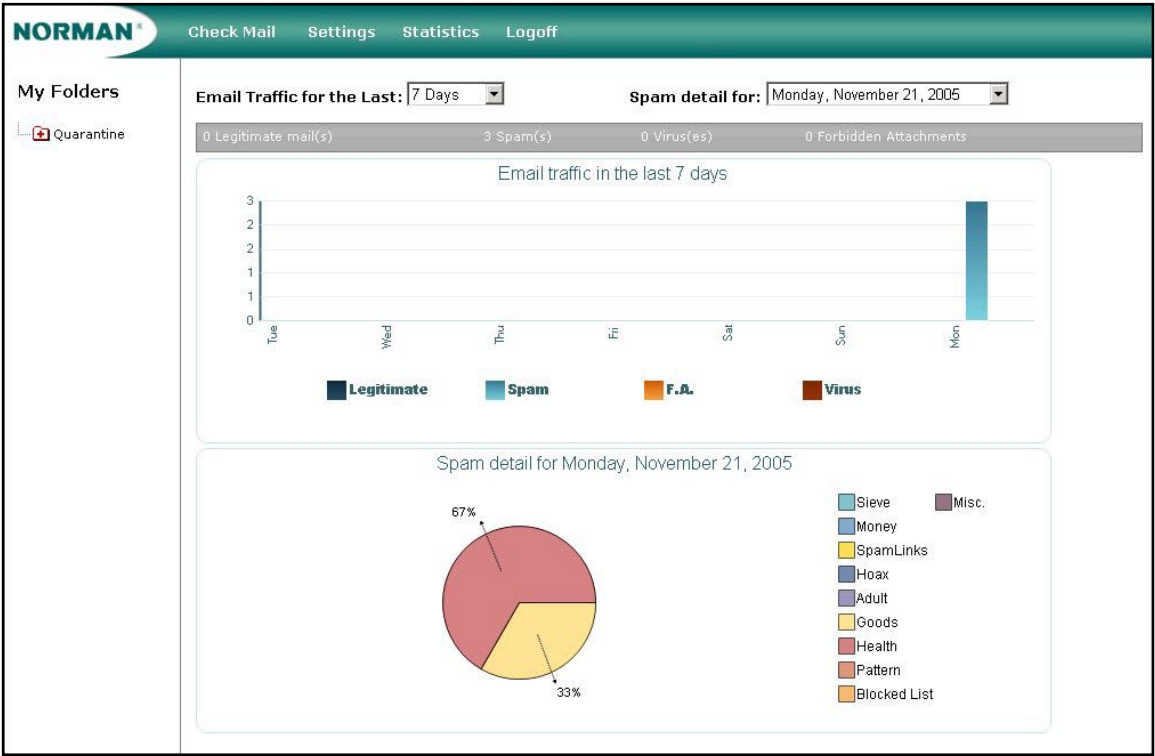
NEP WebQuarantine

**Settings:** The settings menu provides access to the many configuration options you have for how NEP WebQuarantine will manage your mail account. These configuration options include personal settings (password, account identification options, etc) email filtering and sorting options, auto-reply options, external account access, and the creation of aliases for your account.



Settings menu

**Statistics:** This page displays the statistics of your email account's activity.



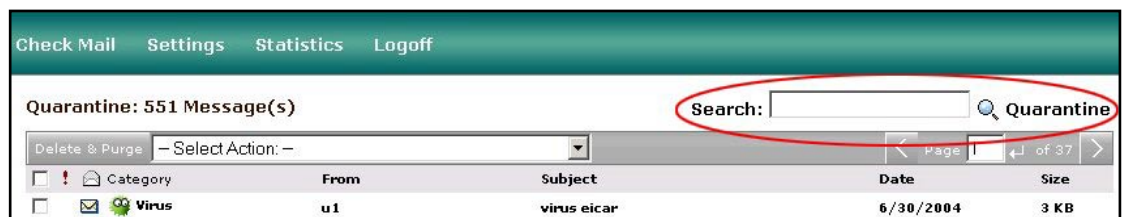
Mailbox Scanning Statistics

## Searching Quarantine

You can search email in your Quarantine.

*NOTE: you can only search across the following criteria (not the body of the message):*

- Subject
  - From
  - To
  - Cc
- Enter your search value and click the magnifying glass



Search Feature

## Paging

For folders that contain many messages, the paging feature allows you to display portions of the message list. The number of messages displayed on each page is configurable, but the default is 15 messages per page. For instructions on how to change this setting, please refer to chapter 3.

### Navigating List Pages

- Select the list page you want to go by clicking either **Next** or **Previous**



Paging Feature

# Chapter 2:

# Quarantine



Email containing attachments that have viruses (or which are attachments that are considered dangerous by the system) cannot be released to your inbox. Only email considered to be spam can be released from Quarantine.

## *Managing Your Quarantined Mail*

The Quarantine feature filters incoming email to determine whether they are spam, or contain forbidden attachments or viruses.

The Quarantine View shows you the name of the sender, the subject of the messages and their attachments. You can also open an email in Quarantine and view its contents; however, you cannot view attachments in Quarantine. Messages in Quarantine can be released to your inbox or deleted and purged from the system.

## Quarantine Categories

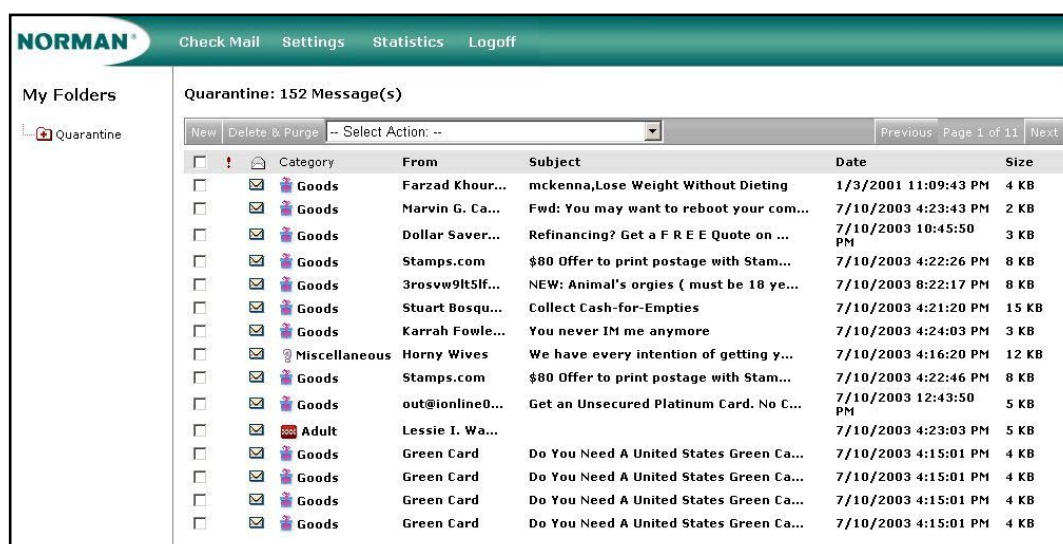
There are 9 categories of mail that can be filtered into Quarantine:



The other categories of email sent to Quarantine are **Virus** or **Forbidden Attachment**. A forbidden attachment is a type of file that your system administrator identifies as being a possible threat.

## False Positives

A False Positive is a message that is identified incorrectly as one of the filtered categories. False positive messages can be released to your Inbox and you can add the email address or domain to your Trusted List so that messages from this source in future will not be Quarantined (unless the system detects a virus).



## Quarantine Contents

### Releasing Email from Quarantine

1. Select the messages you want to release
2. Select either:
  - **Release Message** to just release the message to your inbox

OR

- **Release and Report message as Legitimate** mail to release the message to your inbox as well as sending a copy of it to Norman's Spam-busting team for pattern analysis.



## Deleting and Purging Quarantined Email

You can delete, restore, and purge quarantined email by the same procedures used in other folders. Refer to instructions in *Chapter 2: Email*.



Please see  
**Chapter 5:**  
**Settings** for an  
explanation of how to  
schedule Quarantine Report  
generation.

## Quarantine Reports

NEPMail can be configured to email you Quarantine Reports at regular intervals (typically once a day). You will only receive a Quarantine Report email if you have messages in Quarantine at the time the system generates the reports.

**QUARANTINE REPORT**

This is a spam and virus report sent to recipient@domain.com on Wed Dec 07 10:40:18 2005

**IMPORTANT NOTE.** You are receiving this report because some of the e-mail that was sent to you or from you is suspected to be unsolicited (SPAM) or to contain viruses or other potentially harmful attachments. The suspect messages were neutralized by the server and are actually detained in a private, personal folder called a Quarantine Folder. In case one or more of the e-mails listed below are legitimate messages, you can release them from Quarantine by clicking on the Release link at the right. To remove them permanently from the server, use the individual Delete links or the Delete All links. If viruses or other potentially harmful attachments have been detected, they will be removed from the released message to avoid any damage to your system. In case of doubt or for any question, please contact your [SYSTEM ADMINISTRATOR](#)

If you don't want to receive this report anymore, [click here](#).

---

Your e-mail quarantine folder received: [1 New Viruses](#) --- [1 Viruses](#) --- [1 New Attachments](#) --- [1 Attachments](#) --- [1 New Spam](#) --- [1 Spam](#)

---

Your e-mail quarantine folder received: 1 New suspected virus

**Virus since last report :**

Virus Type	Subject	From	Date	Size	Expiry	Delete
Virus	This is a virus	sender@returnpath.com	Wed Dec 07 11:19:40 2005	1 Kb	N/A	<a href="#">Delete</a>

---

Currently Detained e-mail: 1 virus

**Current quarantined virus:**

Virus Type	Subject	From	Date	Size	Expiry	Delete
Virus	This is a virus	senderWithAstrangelyLongNameThatUsual...	Wed Dec 07 11:19:40 2005	1 Kb	2 day(s)	<a href="#">Delete</a>

[Delete All Virus](#)

Powered by Norman ASA
Questions? Contact your System Administrator
About Norman Email Protection

A Quarantine report shows you information about the email that has been sent to Quarantine since your last report, as well as information about the email that is currently in Quarantine.

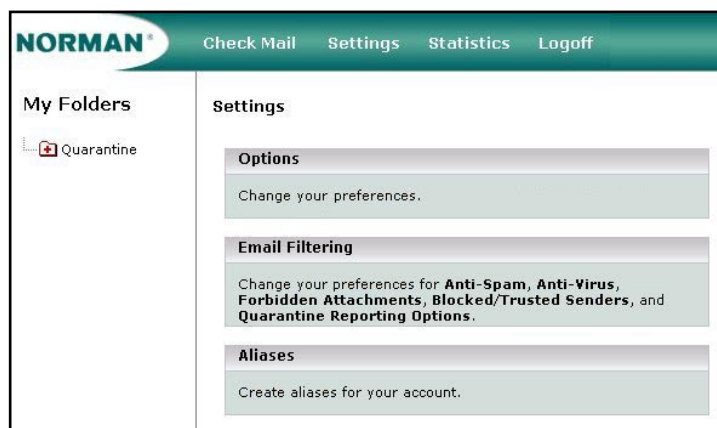
## Releasing or Deleting Quarantined Email from the Quarantine Report

1. Open your Quarantine Report Email View
2. Click the hyperlinks in the report to either:
  - a. **release** the email to your inbox
  - b. **release** the email to your inbox **and report** the email to Norman as a false positive (an email incorrectly identified as illegitimate mail)
  - c. or **delete** the quarantined messages

# Chapter 3:

# Settings

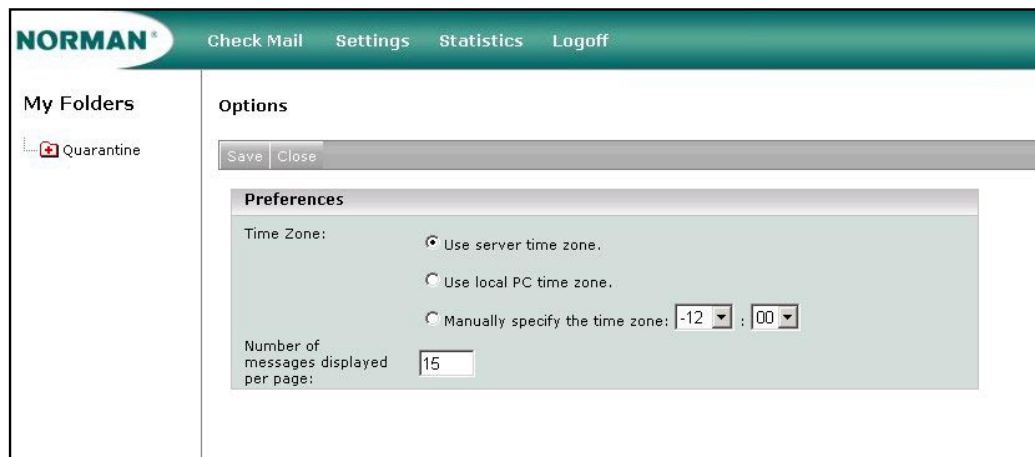
Select **Settings** from the navigation bar to access the pages where you can set preferences for your account's quarantine rules.



Settings Menu

## Options

- Go to **Settings > Options** to set list display preferences.



The screenshot shows the NORMAN web interface. The top navigation bar includes 'Check Mail', 'Settings', 'Statistics', and 'Logoff'. The left sidebar shows 'My Folders' with a 'Quarantine' folder. The main content area is titled 'Options' and contains a 'Save' button and a 'Close' button. Below these is a 'Preferences' section with the following settings:

- Time Zone:**
  - ☒ Use server time zone.
  - ☐ Use local PC time zone.
  - ☐ Manually specify the time zone: -12 : 00
- Number of messages displayed per page:** 15

### Options Settings

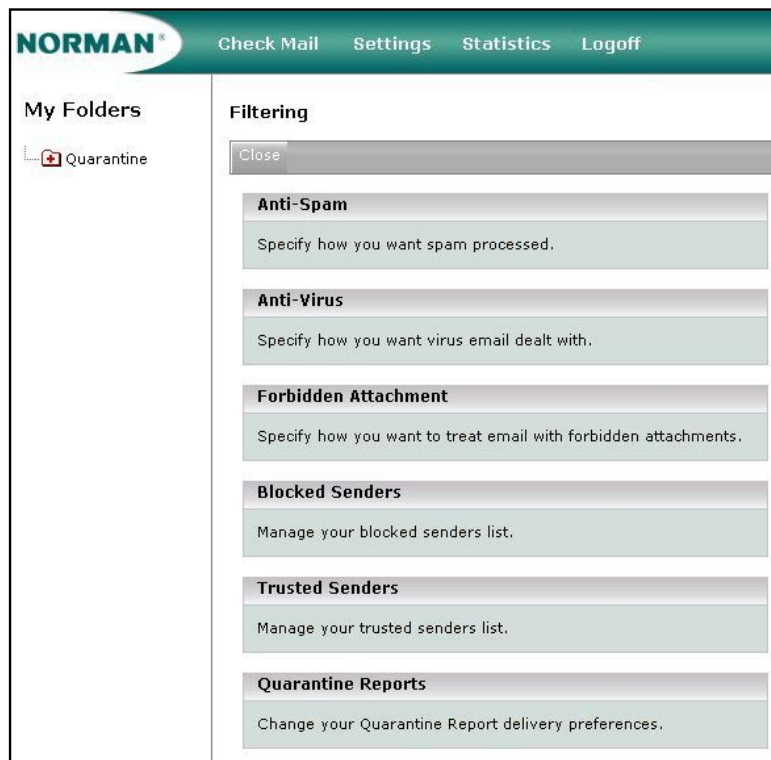
#### Specify the Number of Messages to be Displayed in Lists

1. Choose the time zone you want to use for Message timestamps.
2. Enter the number of messages you want to see on each page
3. Click **Save**

## Email Filters

You can turn on or off, or modify the severity of the filters used to check incoming email for spam, viruses and forbidden attachments.

- Go to **Settings > Email Filtering** to do any of the following procedures



Email Filtering Menu

## Modifying your Anti-Spam Filter Settings

To specify what you want to happen to email identified as spam:

1. Choose either:

- a. Delete message immediately (you will never be able to review messages identified as spam)

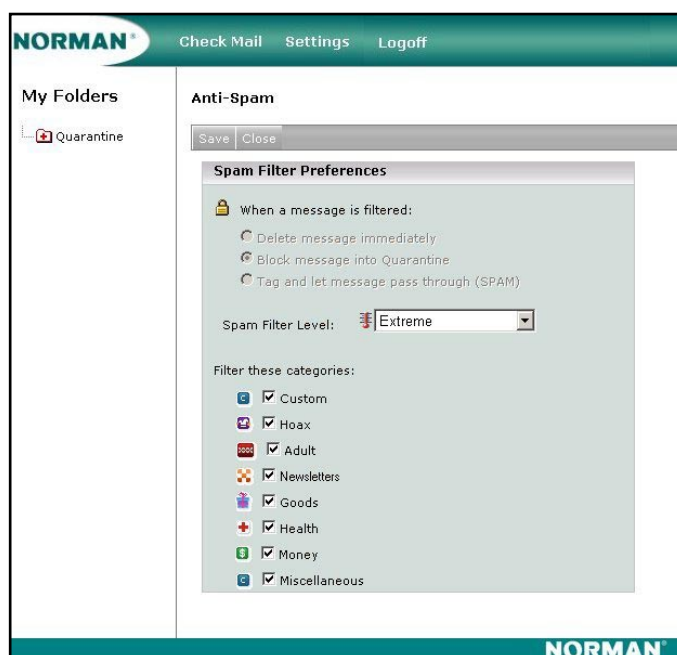
OR

- b. Block message into Quarantine (you will be able to release the message to your inbox)

OR

- c. Tag messages as spam but allow them all through to your inbox

2. Click **Save**



Anti-Spam Filter Settings

To choose the level of Spam Filtering:

1. Choose either:

- a. **Disabled** (no spam filtering)

OR

- b. **Normal** (basic spam filtering)



It is possible that your administrator has made these

settings on your behalf and locked them. In this situation, you will not be able to modify the settings and you must contact your administrator if you want to make changes.

OR

- c. **Strong** (advanced spam filtering used)

OR

- d. **Extreme** (can occasionally result in false positives)

2. Click **Save**

## Modifying your Anti-Virus Filter Settings

To specify what you want to happen to email with viruses, go to **Settings > Email Filtering > Anti-Virus**:

1. Choose either:
  - a. Delete message immediately (you will never be able to review messages that have viruses)

OR

- b. Block message into Quarantine (you will be able to read the message, but not to open any attachment that has a virus)

2. Click **Save**



Anti-Virus settings

## To turn Virus Filtering on or off:

1. Choose either:
  - a. **Normal** to turn on virus filtering

OR

- b. **Disabled** to turn virus filtering off
2. Click **Save**

## To modify Virus notification settings:

1. Choose:
  - **Sender receives notification** to let a sender know that they sent a virus
  - **Recipient receives notification** to let a recipient know that they have email in Quarantine with a virus
2. Click **Save**

## Forbidden Attachments

Forbidden Attachments are defined by the system administrator. Typically a forbidden attachment is a file type that is deemed to pose an unnecessary risk to the system, such as a file with a “.vbs” extension which is commonly used to spread computer viruses via email.

Forbidden attachment settings are modified in the same way that your anti-spam and anti-virus settings are treated, which are explained in the following sections.



Most viruses are now sent from forged email

addresses. So the virus notification option is no longer as effective since the person who receives the notification usually has had nothing to do with it - and potentially that innocent person's inbox could be flooded with virus notifications. Therefore this notification option is not always recommended.



In NEP WebQuarantine you can change your

preferences for the level of restriction for attachments, but you cannot define which file types are to be considered forbidden for each level (normal, strong and extreme) of restriction. Please contact your system administrator if you would like more information about forbidden file types.



## Blocked Senders and Trusted Senders

If you are viewing an email that has been Quarantined, it is easy for you to correctly classify the address of the sender.



Your Trusted List contains the email addresses

of people from whom you always want to receive messages.

Your Blocked List contains the email addresses of people from whom you never want to receive anything.

### Adding Addresses to Your Trusted List

1. Select a message and open the message view
2. Click **Trusted List** to add the sender's address to your Trusted List (this sender's emails will always be sent to your Inbox)

The screenshot shows the NORMAN web interface. At the top, there is a navigation bar with links: Check Mail, Settings, Statistics, and Logoff. On the left, under 'My Folders', there is a 'Quarantine' folder. The main content area is titled 'Trusted Senders'. It features a 'Close' button at the top left. Below it is a section titled 'Add a sender' with an 'Add' button. This section contains two radio buttons: 'Email' (selected) and 'Domain'. Each has a corresponding text input field. Below the input fields, a message states: 'Changes made to your Trusted Sender list may take a few minutes to take effect.' At the bottom, there is a table titled 'Trusted Senders List' with a 'Delete' button. The table contains two entries: 'my\_friend@xyz.com' and 'sales@sinfo.com'.

Trusted Senders List		Delete
<input type="checkbox"/>	my_friend@xyz.com	
<input type="checkbox"/>	sales@sinfo.com	

### Trusted Senders List

## Adding Addresses to Your Blocked List

1. Select a message and open the message view
2. Click **Blocked List** to add this email address to your Blocked List (emails from this address will always either be automatically Quarantined or deleted, depending on the settings the administrator has chosen for the mail server)

The screenshot shows the NORMAN web interface. The top navigation bar includes 'Check Mail', 'Settings', 'Statistics', and 'Logoff'. On the left, under 'My Folders', there is a 'Quarantine' link. The main content area is titled 'Blocked Senders' and contains a 'Close' button. Below this is a 'Preferences' section with a 'Save' button. The preferences include a 'Max. number of entries' field set to '200' and a section for handling blocked messages with three radio button options: 'Delete message immediately', 'Block message into Quarantine' (which is selected), and 'Tag and let message pass through (SPAM)'. Below the preferences is an 'Add a sender' section with an 'Add' button. It has two radio button options: 'Email' (selected) and 'Domain', each followed by a text input field. At the bottom, there is a note: 'Changes made to your blocked sender list may take a few minutes to take effect.' and a message: 'There are no addresses in your Blocked Sender list.'

## Blocked Senders List

## Quarantine Report Settings

You can select the frequency you prefer for receiving a Quarantine Reports if you have been granted rights to override domain and server settings.



Even though you may select to receive a

Quarantine Report each day, you will only receive one IF you have email that is being trapped by the filters and quarantined everyday.

1. Go to Settings > Email Filtering > Quarantine Reporting Options
2. Click **Override my domain defaults** enable the reporting frequency selection
3. Choose the frequency you prefer from the drop-down list



### Quarantine Reporting Options

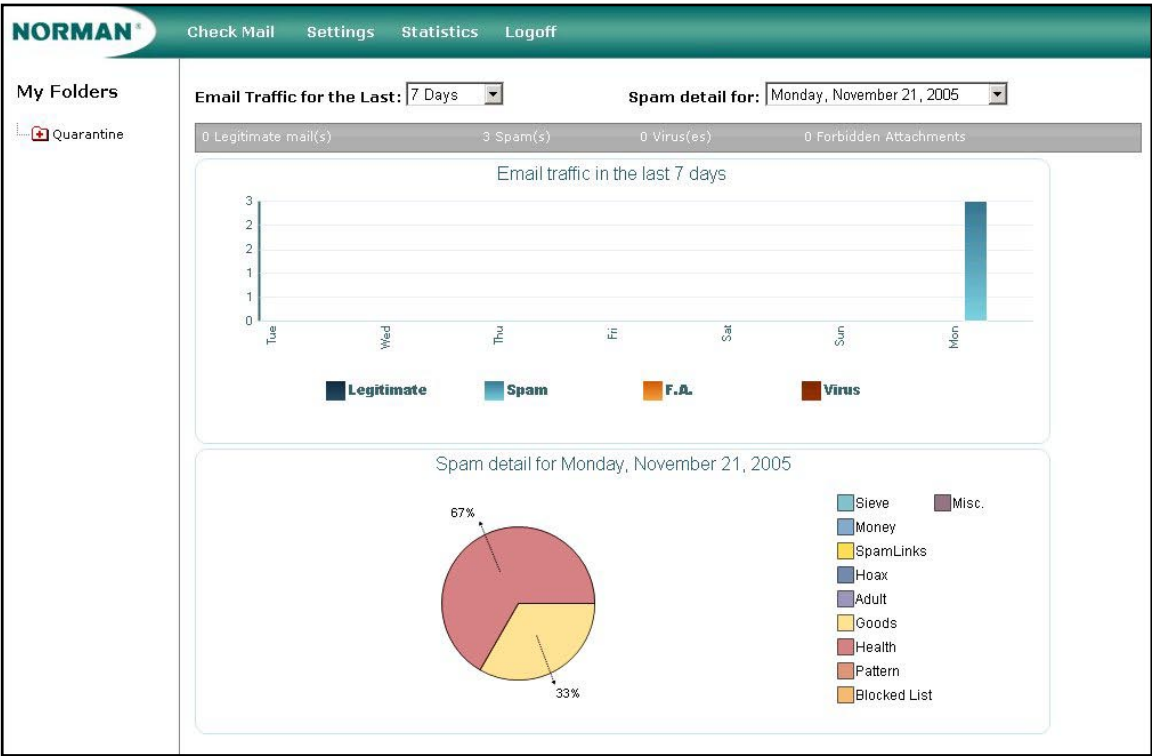
# Chapter 4:

# Statistics

## *Account Statistics*

You can find out what sort of email traffic you've had by checking your homepage. The statistics page has a histogram of daily, weekly, monthly or the last twelve months of information about the amount of legitimate email vs the amount of spam, or email with forbidden attachments or viruses in them that you have received.

You can also see a pie chart of either a daily, weekly or monthly comparison of the different types of spam you've received.



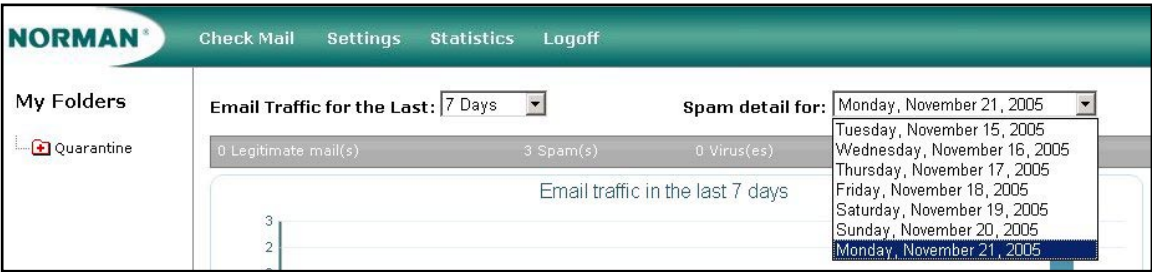
NEP Statistics

## Email Traffic for the Last 7 Days

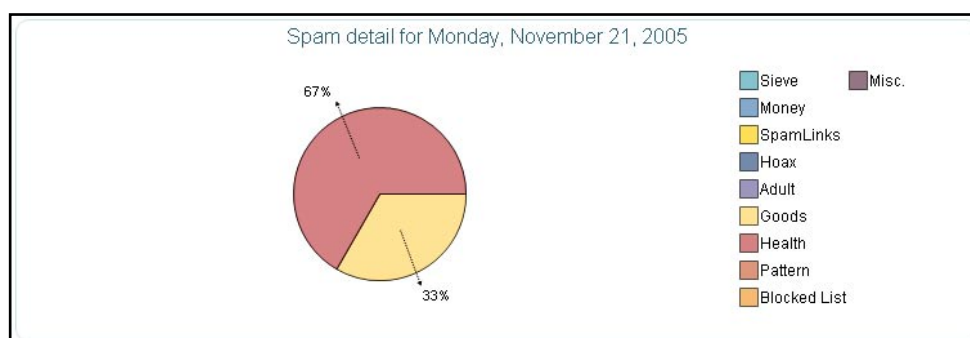
To see a histogram of how many messages you’ve received of legitimate email, spam, email with forbidden attachments and email containing viruses for the last week, select **Email Traffic for the last: 7 Days** from the drop-down list.

### See a daily breakdown of types of spam received

- Select the day whose spam statistics you want to see from the drop-down list.



The pie chart displays the statistics for the categories of spam you received that day.



## Email Traffic for the Last 8 Weeks

To see a histogram of how many messages you've received of legitimate email, spam, email with forbidden attachments and email containing viruses for the last eight weeks, select **Traffic for the last: 8 Weeks** from the drop-down list.

### See a weekly breakdown of types of spam received

- Select **Email Traffic for the last: 8 Days** from the drop-down list.
- Select **Spam detail for the week of: <date>** for the week you want to see from the drop-down list.

The pie chart displays the statistics for the categories of spam you received that on a weekly basis.

## Email Traffic for the Last 12 Months

To see a histogram of how many messages you've received of legitimate email, spam, email with forbidden attachments and email containing viruses for the last twelve months, select **Traffic for the last: 12 Months** from the drop-down list.

### See a monthly breakdown of types of spam received

- Select **Email Traffic for the last: 12 months** from the drop-down list.
- Select **Spam detail for the month of: <date>** for the month you want to see from the drop-down list.

The pie chart displays the statistics for the categories of spam you received that month.

# Glossary

## Alias

An alternate name given to a mailbox.

## Auto-Reply

An email message that is to be sent out automatically in response to any email received.

## BCC (Blind Carbon Copy or Blind Courtesy Copy)

Recipient(s) in this list on an email are not displayed and are not visible to the direct or carbon-copied recipient(s) of an email.

## Blacklists

See *Blocked List*

## Blocked List

Allows users to designate a domain or IP address and email addresses from which no mail will be accepted.

## Browser (also Web Browser)

This is a software application that allows you to view (or “browse”) and interact with web sites on the internet. Some of the most common web-browsing software applications are Microsoft Internet Explorer, Netscape Navigator, Mozilla Firefox, Opera and Safari.



## Browser Compatibility

The term “browser compatibility” refers to the fact that web-browsing applications from different companies sometimes display the same web pages with different formatting. This is to say that they interpret the code behind a web page (code which consists of HTML tags) differently. Sometimes these differences are minimal, but unfortunately these interpretational differences can sometimes also mean that you simply cannot view some parts of a website that has used particular HTML code tags because your web browser does not know how to display those parts (which use specific HTML tags).

## CC (Carbon Copy or Courtesy Copy)

Recipient(s) in this field of an email’s address list are not the direct recipients of the email. CC Recipients of an email are generally not required to take action on it, and their inclusion is usually for informational purposes only.

## Catch Rate

The percentage of spam mail caught by a spam solution. It measures the efficiency of the solution at identifying and stopping spam.

## Content filtering

Scans plain text for key phrases and the percent of HTML, images and other indications that the message is spam.

## CSV (Comma Separated Values)

This is a comma-delimited text file.

## Dial-up Internet Account

This is an account that allows you to use a modem to connect to an internet service provider who then gives you direct access to the internet.

## False Negative

A false negative is an email that is spam, but which was not recognized by an anti-spam solution and was released to your inbox as legitimate email.

## False Positive

A false positive is a legitimate email, but which was recognized by an anti-spam solution wrongly as spam email and withheld from your inbox.

## ISP (Internet Service Provider)

A company that provides a connection to the Internet.

## Quarantine

To isolate files suspected of containing a threat such as a virus, so that it can not be opened.

## Quarantine Report

A report of a NEPMail account's quarantined email that is sent to a user's inbox at regular intervals. This report is only generated when a user's account has email that has been identified either as spam or containing a virus and which has accordingly been withheld from the user's inbox.

## Server

A computer that runs administrative software (for the purposes of this user guide, a server is a computer on the internet that runs an email exchange program).

## Spam

Unsolicited, unwanted, bulk, commercial e-mail.

## Trusted Sender List

Lets users designate a source or IP address from which all mail will be accepted, even if individual messages earn high spam ratings.

## URL (Universal or Uniform Resource Locator)

This is an internet address used by web browsers for a specific computer or a document (resource).

## Whitelists

See *Trusted List*